DOCKET: CU-5069

***IN THE UNITED STATES PATENT & TRADEMARK OFFICE***

APPLICANT: Li LIU

SERIAL NO: 11/521,254

FILING DATE: September 14, 2006

TITLE: METHOD FOR MANAGING A VIRTUAL PRIVATE NETWORK

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

***SUBMITTAL OF PRIORITY DOCUMENT***

Dear Sir:

Attached herewith is a certified copy of Chinese Application 2004 10044310.X filed May 21, 2004, for which priority is claimed under 35 USC 119.

Respectfully submitted,

December 4, 2006
Date

Attorney for Applicant

/2

Brian W. Hameder, Reg. 45613
c/o Ladas & Parry LLP
224 South Michigan Avenue
Chicago, Illinois 60604
(312) 427-1300

中华人民共和国国家知识产权局
STATE INTELLECTUAL PROPERTY OFFICE
OF THE PEOPLE'S REPUBLIC OF CHINA

# 证　　明

本证明之附件是向本局提交的下列专利申请副本

申　　请　　日：2004.05.21

申　　请　　号：200410044310.X　　OP0677131PIUS

申　请　类　别：发明专利

发明创造名称：虚拟专用网网络管理方法

申　　请　　人：华为技术有限公司

发明人或设计人：刘黎

中华人民共和国
国家知识产权局局长　田力普

2006 年 10 月 8 日

# 权　利　要　求　书

1. 一种虚拟专用网网络管理方法，其特征在于，所述方法包含以下步骤：

A 网管系统搜集网络中所有虚拟专用网的状态信息；

B 根据搜集到的每一个虚拟专用网的状态信息，在所述网管系统的监控终端上用不同颜色的图标表示该虚拟专用网；

C 把告警和故障信息用文字形式显示在代表相应虚拟专用网的图标上。

2. 根据权利要求 1 所述的虚拟专用网网络管理方法，其特征在于，每一个所述图标对应一个虚拟专用网或一组虚拟专用网。

3. 根据权利要求 1 所述的虚拟专用网网络管理方法，其特征在于，当所述监控终端收到向一个所述图标发送的命令时，所述网管系统以该图标对应的一个或一组虚拟专用网为对象进行操作。

4. 根据权利要求 1 所述的虚拟专用网网络管理方法，其特征在于，所述方法还包含以下步骤：

在所述网管系统中预先设定所述图标的颜色和所述虚拟专用网状态的对应关系。

5. 根据权利要求 2 所述的虚拟专用网网络管理方法，其特征在于，当一个所述图标对应一组所述虚拟专用网，而该组中的虚拟专用网处于至少两个不同严重程度的状态，则所述图标的颜色反映最严重的状态。

# 说　明　书

## 虚拟专用网网络管理方法

### 技术领域

本发明涉及通信系统中的网管技术，特别涉及用虚拟专用网的网管技术。

### 背景技术

虚拟专用网（Virtual Private Networking，简称“VPN”）指的是依靠电信运营商、因特网服务提供商（Internet Service Provider，简称“ISP”）、网络服务提供商（NetWork Service Procider，简称“NSP”）等（以下统称供应商），在公用网络中建立专用的数据通信网络的技术。在 VPN 中，任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是利用某种公众网的资源动态组成的。所谓虚拟（Virtual），是指客户不再需要拥有/租用实际的长途数据线路，而是使用供应商网络的各种数据线路。所谓专用（Private），是指仅该客户占用该网络，而其他客户无法访问/占用该网络。VPN 的实现技术有很多，例如，二层隧道协议（Layer 2 Tunnel Protocol，简称“L2TP”）、网际协议安全（InternetProtocol Security，简称“IPSec”）、通用路由封装（Generic Route Encapsulation，简称“GRE”）、边界网关协议（Border Gateway Protocol，简称“BGP”）/多协议标签交换（MultiProtocol Label Switching，简称“MPLS”） VPN 等。

由于 VPN 是在供应商的一个网络上，模拟地实现出租给客户的多个网络，因此供应商在网络管理、业务监控时，就存在一定的复杂性：

同一设备或链路可能会同时租用给多个客户，则该物理设备或链路出现故障，就会同时影响多个客户租用的虚拟专用网。

同一客户租用的虚拟专用网可能有有 2 个或 2 个以上的站点，任何单一

设备或链路的状态都无法决定整个虚拟专用网的运行状态。

同一供应商会同时管理多个客户的多个虚拟专用网，就必须要很方便地监控所有的虚拟专用网。

图 1 示出了采用 BGP/MPLS VPN 技术实现的 VPN 结构，其中包括两个 VPN:

集团 1 包含站点 31、33、35;

集团 2 包含站点 32、34。

假定 PE 21 宕机，则集团 1、集团 2 两个 VPN 都会发生问题；再假设 PE 22 与 CE 43 相连的链路虽然是正常的，但 PE 23 与 CE 45 相连的链路却是故障的，则集团 1 也会出现问题。由此可见，网络中任何单点故障或正常都不能反映实际某个 VPN 的运行状况。

现有 VPN 网管系统/VPN 业务管理系统，就是定位于管理网络中各客户的 VPN，包括 FCAPS 五大功能（Fault 告警、Configuration 配置，Accounting 计费、Performance 性能、Security 安全）。与通常的网管系统和业务管理系统类似，拓扑功能也是 VPN 网管系统/VPN 业务管理系统必不可少的特性。所谓拓扑功能，是指以图形方式显示网络各节点之间相互连接的形式，这是供应商管理在进行网络的一个最基本、最常用功能之一。

现有 VPN 网管系统/VPN 业务管理系统中，已有的拓扑显示方法通常就是供应商视图（Provider's view）和客户视图（Customer's view）两种。

供应商视图：提供 CE 设备与 PE 设备之间的连接关系的拓扑视图。从供应商的角度来看，客户的站点/CE 是连接到供应商网络中的 PE 设备上的，而且全网提供的 VPN 也是很多个（每个客户可能仅租用一个 VPN，也可能是一个客户同时租用多个 VPN）。通常网络视图既可以提供全网的视图，也可以提供按客户来过滤的客户视图。图 2 示出了两个集团各租用了一个 VPN 的

供应商视图。

客户视图：提供 CE 设备与 CE 设备之间的虚拟连接关系的拓扑视图。从客户的角度来看，他们认为自己的网络就是从一个站点/一个 CE 直接连接到另外一个站点/另外一个 CE 的，即好像 CE 设备之间是直接相连的。虽然物理网络的实际流量是需要穿越供应商提供的中间网络的。通常客户视图都是按客户来查看的，图 3 示出了集团 1 租用的 VPN 的客户视图，它表达了集团 1 在三个办公地点之间的连接关系。客户视图也可以按照多个客户一起查看，不过这仅仅在多个客户之间存在 Extranet 的情形下才有意义。

比较供应商视图和客户视图，可以看到：

供应商视图的侧重点在于提供全网 CE 挂接方式的图形化显示方式，即哪个 CE 是挂接到哪个 PE 上的，其优点是能够提供 VPN 挂接点的整网视图。

客户视图的侧重点在于提供客户 CE 之间的拓扑连接关系，其优点在于对于客户而言简化了中间网络，便于了解客户的虚拟组网情况。

然而，在实际应用中，无论是供应商视图还是客户视图都有一个共同的缺点——无法对当前全网所有 VPN 的状况（告警、流量、性能）有一个一目了然的图形显示。

在普通网络管理（不包括 VPN 特性时）的实际应用过程中，网络管理人员可能会长期打开整网的拓扑视图，通过这个界面来了解当前网络的运行状况。但是由于 VPN 网络场景下 VPN 的特殊性和复杂性，导致无论是供应商视图，还是客户视图，都无法给网络管理人员一个当前全网所有 VPN 的状况一目了然的答案。

所谓 VPN 状况，不仅仅包括设备上报的告警信息，还包括网管系统主动轮询得到的流量、性能数据，这些都是影响客户使用该 VPN 的情况。

例如，在 BGP/MPLS VPN 情况下，某台 PE 设备的 VRF 路由表越限并

发送告警给 VPN 网管系统/VPN 业务管理系统，这说明在一段时间后如果路由表项数量继续增加，则可能导致使用该 VRF 的 VPN 客户在访问后续增加的目的网段时将无法到达。这种情况无法在客户视图中表达（因为其中根本没有 PE），也不好在供应商视图中表达，虽然供应商视图中，可以把对应的 PE 设备变成故障状态，但因为同一 PE 可能会接入多台 CE，某个 VRF 路由表越限只影响使用该 VRF 的 VPN 客户，而并不影响使用该 PE 的 VPN 客户，把 PE 设备变成故障状态会误导成该 PE 下挂接的所有 CE 都会受到影响。

又如，在 BGP/MPLS VPN 情况下，某两台 PE 之间的 BGP 对等体连接出现问题，则会导致路由丢失，即这两台 PE 下挂接的需要互联的 CE 之间无法互通。这种情况无法在客户视图中表达（因为其中根本没有 PE），也不好在供应商视图中表达，因为其中不表达 BGP 对等体的状态。但这种问题却会直接影响 VPN 的连通性状态。

又如，在 MPLS VPN 情况下，某台 P 设备（骨干网路由器）故障可能导致 PE－PE 之间的 LSP 出现问题，这也会导致 VPN 连通出现问题。这种情况无法在客户视图和供应商视图中表达（因为其中根本不包括 P 设备）。

再如，VPN 内部从一个站点到另外一个站点之间流量越限，可能会导致供应商网络流量增加、带宽资源减少。这种情况无法在供应商视图中表达，因为其中不包括 CE－CE 之间的连接状况；的确在客户视图中表达很合适，但是一个供应商网络可能会同时提供多个 VPN（例如，上百的规模），同一界面内把所有 VPN 的客户视图都显示出来是无法做到的。

总之，产生以上问题的原因可以归结如下：

第一，因为供应商视图、客户视图能够表达的状态信息仅仅局限在 PE 设备、CE 设备、PE 与 CE 之间的链路这三个对象，而实际影响 VPN 状态的远不只这三者。

第二，客户视图很难提供全网所有 VPN 一览图，因为网络中 VPN 的数

量和规模（可能会到数百甚至更大）很大，以每个 VPN 平均包括四个站点、每个 CE 图标使用 32*32 像素来计算，则显示一个 VPN 客户视图就需要 9*32*32 的屏幕空间（因为每个图标之间要留出画连线的空间），那么以常用的显示器分辨率 1024*768 来计算（忽略系统通常有的菜单、状态、窗口边框等空间），则整屏最多可同时容纳 85 个 VPN。而实际有些规模较大的 VPN（例如，一些跨国集团公司），其中可能包括的站点可能就达几百。

第三，供应商视图虽然可显示整网的 PE－CE 连接情况，但是 VPN 的概念含量比较少，很难在此拓扑视图中确定哪些因素、设备、链路是归属于哪些 VPN 的。

另外的一种现有技术就是，完全不考虑 VPN 环境的特殊性，直接显示原有网管系统中的拓扑视图——传统的拓扑视图，例如 IP 拓扑视图。

这种现有技术的问题在于传统的拓扑视图不体现 VPN 的任何信息，没有客户的概念，所以也不能满足 VPN 场景下的，网络管理、监控的需求。

## 发明内容

有鉴于此，本发明的主要目的在于提供一种虚拟专用网网络管理方法，使得网络管理人员可以快速了解、监控现网运行的全部 VPN 状态。

为实现上述目的，本发明提供了一种虚拟专用网网络管理方法，所述方法包含以下步骤：

A 网管系统搜集网络中所有虚拟专用网的状态信息；

B 根据搜集到的每一个虚拟专用网的状态信息，在所述网管系统的监控终端上用不同颜色的图标表示该虚拟专用网；

C 把告警和故障信息用文字形式显示在代表相应虚拟专用网的图标上。

其中，每一个所述图标对应一个虚拟专用网或一组虚拟专用网。

当所述监控终端收到向一个所述图标发送的命令时，所述网管系统以该

图标对应的一个或一组虚拟专用网为对象进行操作。

所述方法还包含以下步骤：

在所述网管系统中预先设定所述图标的颜色和所述虚拟专用网状态的对应关系。

当一个所述图标对应一组所述虚拟专用网，而该组中的虚拟专用网处于至少两个不同严重程度的状态，则所述图标的颜色反映最严重的状态。

通过比较可以发现，本发明的技术方案与现有技术的区别在于，网管系统搜集所有 VPN 的信息后，根据每一个 VPN 的状态使用不同颜色的图标显示在网管终端上，其中每一个图标对应一个 VPN 或对应一组至少有一个共性的 VPN，同时把故障原因等信息以文字形式显示在相应的图标上；当网管人员向一个图标发送命令时，网管系统对该图标对应的一个或一组 VPN 进行操作。

这种技术方案上的区别，带来了较为明显的有益效果，即网络管理人员可以快速、全面地了解现网运行的全部 VPN 状态，并能够及时、方便地对发生故障的 VPN 进行处理。以下举例说明：

在 BGP/MPLS VPN 情况下，某台 PE 设备的 VRF 路由表越限并发送告警给 VPN 网管系统/VPN 业务管理系统，这说明在一段时间后如果路由表项数量继续增加，则可能导致使用该 VRF 的 VPN 客户在访问后续增加的目的网段时将无法到达。这种情况就将该 VRF 对应的 VPN 的节点变红（若有必要可上传到其父节点）即可。

在 BGP/MPLS VPN 情况下，某两台 PE 之间的 BGP 对等体连接出现问题，则会导致路由丢失，即这两台 PE 下挂接的需要互联的 CE 之间无法互通。这种情况，可以把与依赖于这个对等体连接的所有 VPN 的节点颜色变红（若有必要可上传到其父节点）即可。

在 MPLS VPN 情况下，某台 P 设备故障可能导致 PE－PE 之间的 LSP 出现问题，这也会导致 VPN 连通出现问题。这种情况可以把使用到该 LSP 的所有 VPN 的节点颜色变红。

VPN 内部从一个站点到另外一个站点之间流量越限，可能会导致供应商网络流量增加、带宽资源减少。这种情况可以把该 VPN 的节点颜色变红。

**附图说明**

图 1 是采用 BGP/MPLS VPN 技术实现的 VPN 的结构示意图；

图 2 是现有技术中 VPN 的供应商视图；

图 3 是现有技术中 VPN 的客户视图；

图 4 是根据本发明的一个实施例的 VPN 网络管理方法流程图；

图 5 是根据本发明的一个实施例的 VPN 网络显示结果示意图；

图 6 是根据本发明的一个实施例的 VPN 网络分类分层显示结果示意图。

**具体实施方式**

为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述。

如图 4 所示，VPN 网络管理方法包含以下步骤：

在步骤 110 中，网管系统搜集所有 VPN 的信息。搜集方式可以是网管主动查询或被动地接受上报消息。例如网管系统可以定时对所管辖的所有 VPN 站点发送查询命令，VPN 站点收到查询命令以后发送本站点的状态信息给网管系统。又如，当一个 VPN 站点发生了 VPN 连通信故障，该站点主动向网管系统发送告警信息。

此后进入步骤 120，网管系统根据每一个 VPN 的状态使用不同的颜色显示在网管操作终端上。本发明采用以 VPN 为对象的拓扑显示方法，即以 VPN

作为拓扑显示对象、显示元素。在 VPN 网管系统中，这是一种创新的拓扑显示方法。

其显示效果大致如图 5 所示，拓扑视图以 VPN 作为拓扑显示的基础，每个 VPN 站点使用一个图标来显示，利用图标的颜色来表示当前该 VPN 的状态（不同的颜色代表不同的故障级别，例如，黄色表示一般故障、红色表示重要故障。在图 5 中，因为附图无法表示颜色，因此采用不同的填充模式来替代不同的颜色）。至于具体什么样的状态需要对应是么样的颜色，则可以由系统开发人员或网络管理人员在系统中预先设定。

如果网络规模较大一个界面显示不完，或者希望把现网中的 VPN 进行分类显示，则还可以采用分层、分类的显示形式。这种分层分类实质上是用一个图标对应一组至少有一个共性的 VPN。具体如何分层分类，可以按照网络管理人员的意愿进行划分。例如，

按照地域来分，例如，可分为华东、华中、华北等片区；这样可以轻松的划分不同管理权限的网管人员的不同管理权限。

按照客户等级来分，例如，可分为金牌 VPN、银牌 VPN、铜牌 VPN；这样对于不同等级客户 VPN 的故障处理速度也可以区别对待。

这种分层、分类的显示方法是可以嵌套的。例如，可以先按照地域来划分、再按照客户等级来划分；也可以按照大的地域来划分、在按照小的地域来划分、层层迭代（理论上是可以无穷层的，但从易用性上来讲 2～3 层是比较合适的）。例如在图 6 中，把全网划分为 4 个 VPN 组，每个 VPN 组的图标颜色是根据其下所包括的 VPN 的颜色计算得来的。这种方式可以让 VPN 管理人员，轻松的打开这钟顶层拓扑视图，即可了解全网所有 VPN 的状态。

在分层分类的情况下，如果某一个 VPN 发生故障，该 VPN 以上的所有层次都应该显示该故障。例如，整个网络被划分为 4 个 VPN 组，第一个 VPN 组中又包含 3 个 VPN 小组。则当第一个 VPN 小组中的一个 VPN 发生故障时，

第一个 VPN 小组和第一个 VPN 组的图标都应该转变为代表故障的红色。此时如果网管终端上只显示第一层的 4 个 VPN 组，则代表第一个 VPN 组的图标应该显示为红色，其对应的文字信息显示发生故障的 VPN 的故障原因。如果网管人员进入下一层，则代表第一个 VPN 小组的图标显示为红色。

在分层分类的情况下，如果一个图标对应多个 VPN，而这多个 VPN 出现了不同等级的告警和故障，例如其中一个 VPN 应该显示黄色的告警，另一个 VPN 应该显示更严重的红色故障，此时图标颜色应该显示该图标所对应的 VPN 中最严重的状态，也就是说，在上述例子中，该图标应该显示红色。

此后进入步骤 130，网管系统把 VPN 故障或告警信息采用文字形式显示在该 VPN 对应的图标上。这样做的好处是网管人员可以在通过颜色知道某一个 VPN 发生故障的同时还可以通过文字信息快速了解故障原因。例如，当图 5 中的 VPN－h 发生 VPN 连通性故障的时候，VPN－h 把故障信息发送到网管系统，网管系统把该 VPN 对应的图标设置为红色（表示发生故障），然后把收到的故障信息的内容显示在 VPN－h 的图标上，可以参见图 5 的样式。熟悉本发明领域的技术人员会理解，可以采用其他的故障信息显示方式，例如当鼠标移动到该图标时才显示故障信息等等，而不会超出本发明的实质和范围。

除了故障信息，需要引起网管人员重视的其他信息也可以显示，例如图 5 中，VPN－c 带宽利用率超过了预先设定的阈值，因此也可以显示在 VPN－c 对应的图标上。

在分层分类的情况下，如果一个图标对应多个 VPN，则该图标对应的所有 VPN 的告警和故障信息都会显示在该图标上。如果需要显示的内容过多，可以优先选择最重要的信息显示。

此后进入步骤 140，当网管人员在网管操作终端上向一个图标发送命令时，网管系统对该图标对应的一个或一组 VPN 进行操作。

在本发明的一个较佳实施例中，在每个 VPN 图标上可提供相关操作的右键菜单，例如，查看相关告警、查看客户视图、查看供应商视图、查看性能报表。当网管人员选择了相应的菜单，则网管系统向该图标对应的一个或一组 VPN 发送该菜单所对应的操作，如果该操作有反馈信息，则可以将反馈信息显示在网管终端上。

还需要说明的是，由于大部分客户可能只会申请一个 VPN，所以在 VPN 场景下，也可以采用以客户为对象的拓扑显示方法。对于一个客户申请了多个 VPN 的情况，就只好把一个客户虚拟地看成多个子客户来处理，最终实现一个客户对应一个 VPN 的目的。

虽然通过参照本发明的某些优选实施例，已经对本发明进行了图示和描述，但本领域的普通技术人员应该明白，可以在形式上和细节上对其作各种各样的改变，而不偏离所附权利要求书所限定的本发明的精神和范围。

# 说 明 书 附 图

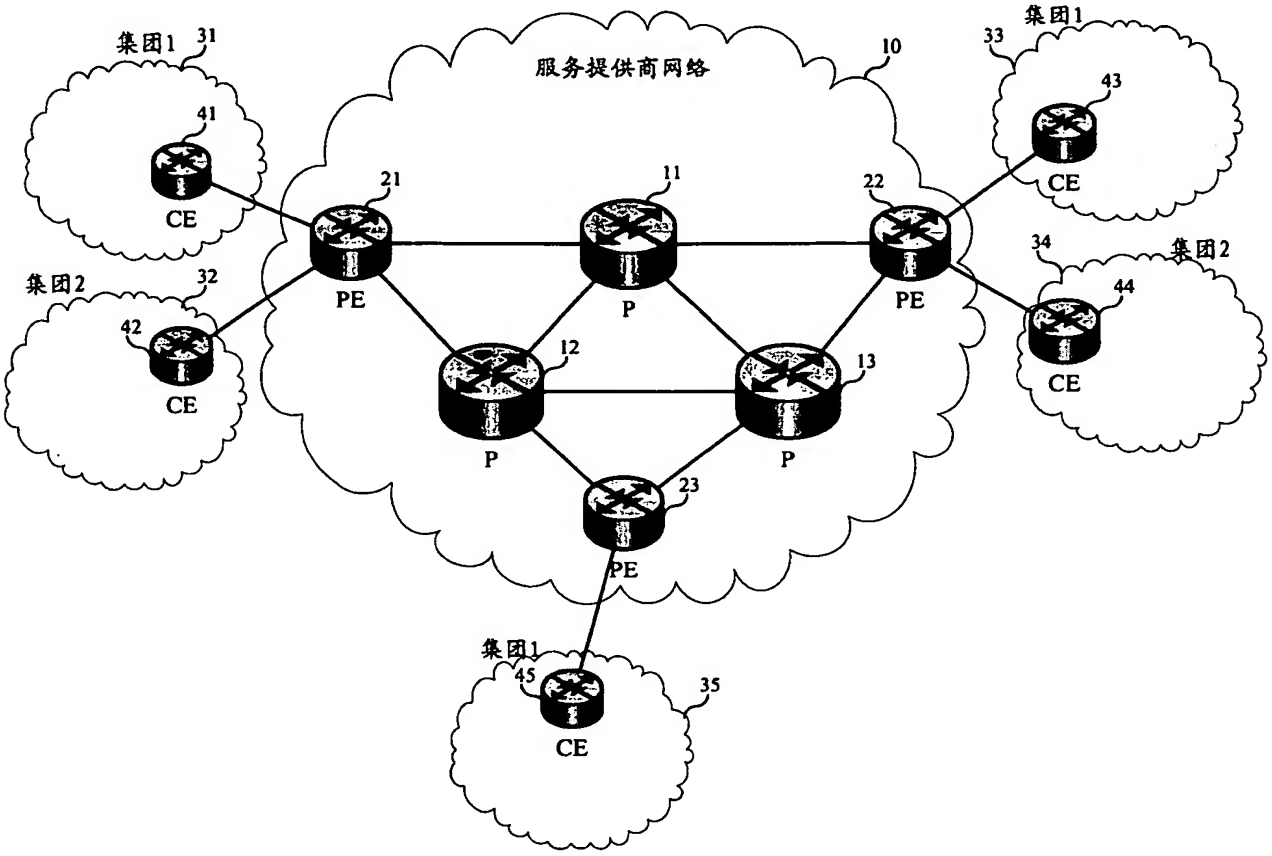
集团1
31
服务提供商网络
10
集团1
33
41
43
CE
CE
21
11
22
集团2
34
集团2
32
44
42
PE
P
PE
CE
CE
12
13
P
P
23
PE
集团1
45
35
CE

图 1

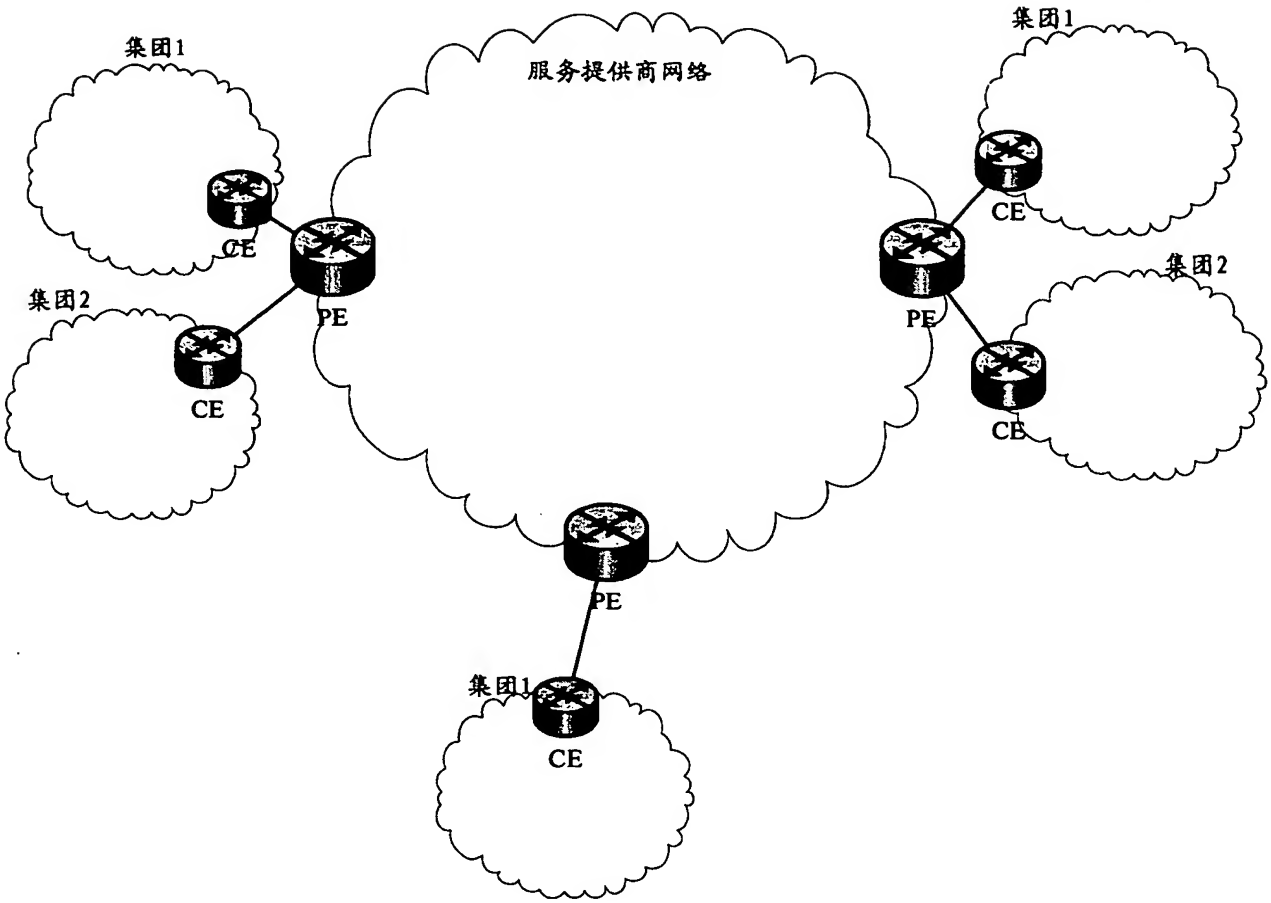
集团1
服务提供商网络
集团1
CE
CE
集团2
PE
PE
集团2
CE
CE
PE
集团1
CE

图 2

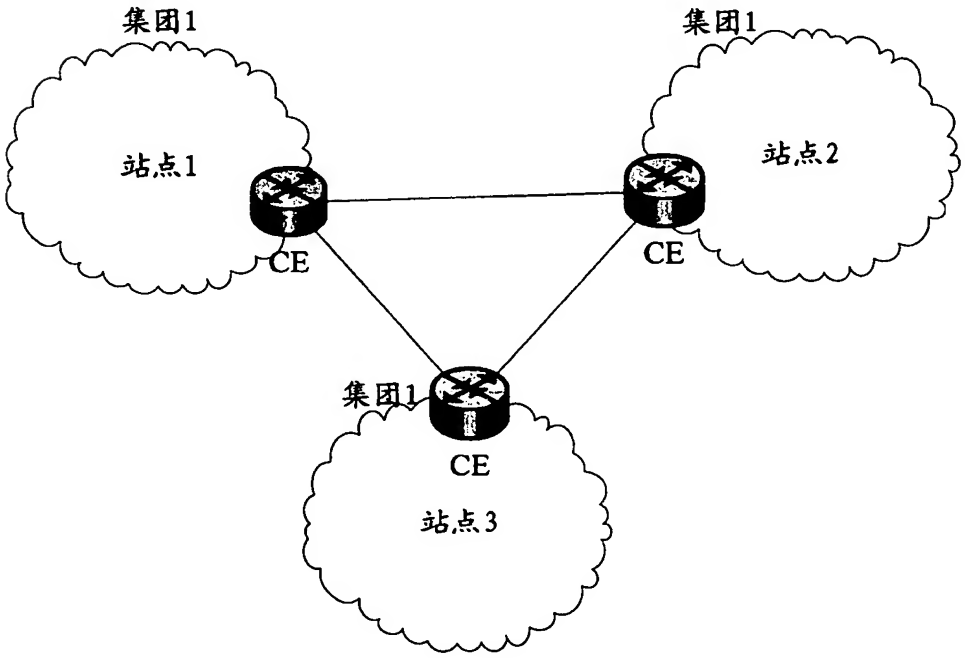
集团1
集团1
站点1
站点2
CE
CE
集团1
CE
站点3

图 3

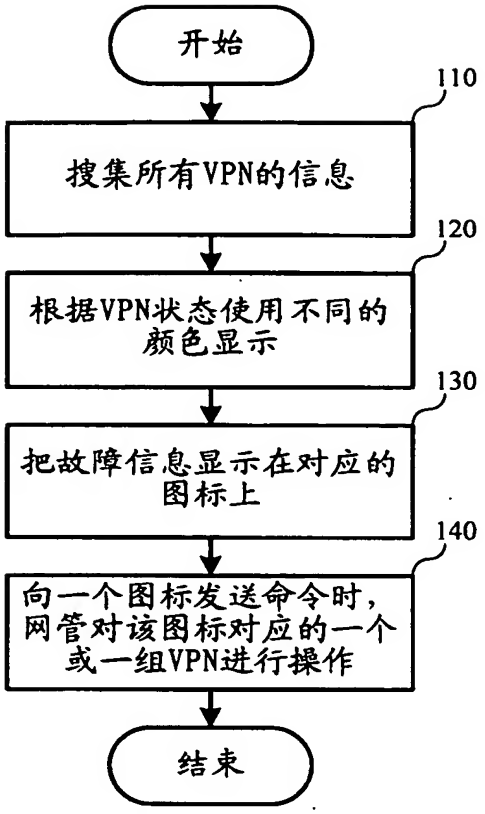
开始
110
搜集所有VPN的信息
120
根据VPN状态使用不同的颜色显示
130
把故障信息显示在对应的图标上
140
向一个图标发送命令时，网管对该图标对应的一个或一组VPN进行操作
结束

图 4

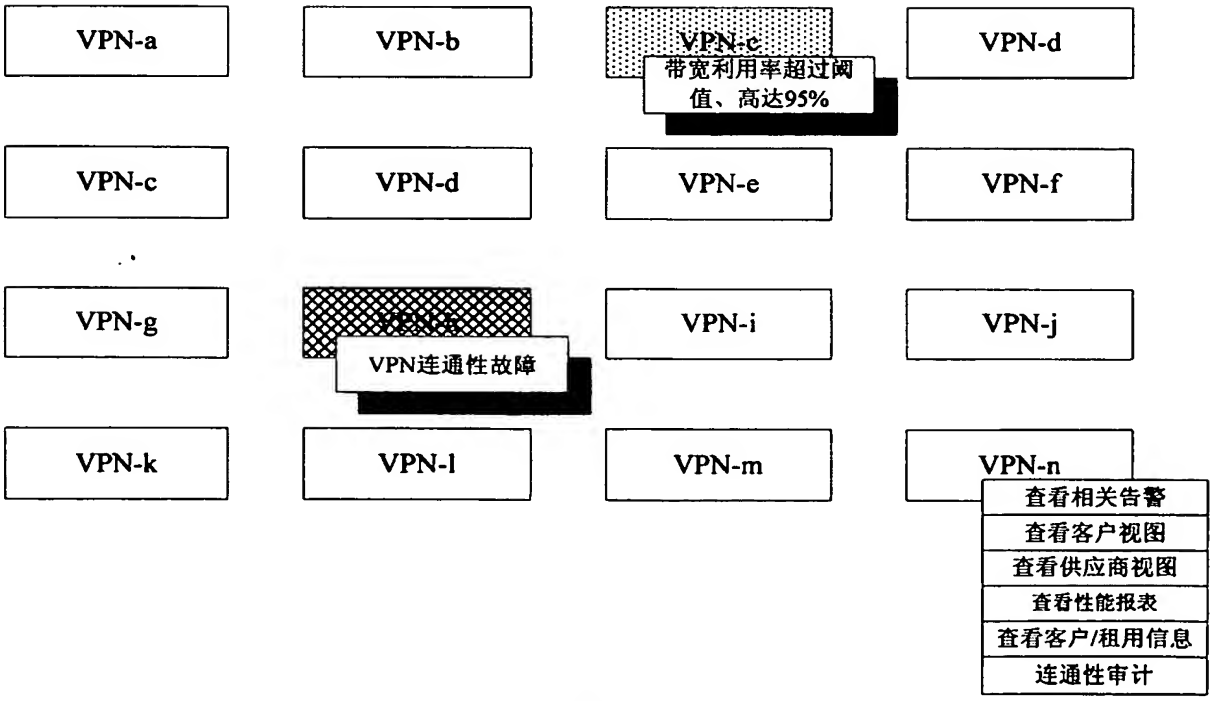
VPN-a
VPN-b
VPN-c
带宽利用率超过阈值、高达95%
VPN-d
VPN-c
VPN-d
VPN-e
VPN-f
VPN-g
VPN-i
VPN-j
VPN连通性故障
VPN-k
VPN-l
VPN-m
VPN-n
查看相关告警
查看客户视图
查看供应商视图
查看性能报表
查看客户/租用信息
连通性审计

图 5

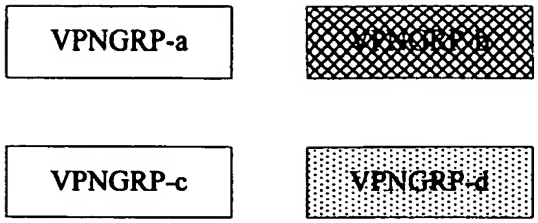


图 6